REMARKS

Claims 1-14 and 15-43 were pending at the time of the Office Action of 23 April 2008, in which all were finally rejected. Claim 13 was previously cancelled. In this Response Accompanying Request for Continued Examination, applicant has amended claims 14, 26, 31, 34, 36, 37 and 39. New dependent claims 44 and 45 are presented.

New claims.

New dependent claims 44 and 45 are added. Each claim is supported in the specification at page 8, line 27 to page 9, line 7 and page 11, lines 4 to 13.

Rejections under 35 USC 112, second paragraph

Applicant respectfully disagrees with the Examiner's view that claims 39 and 40 are not disclosed in the written description in a manner that reasonably conveys to one of ordinary skill how (as now amended) "the at least one client device is adapted to receive separately the first part of the authorisation data and the mobile device identity information from the mobile device."

Claim 39 relates to the situation where the at least one client device (Tagboard box 100) is adapted to receive separately the first part of the authorisation data and the mobile device identity information from the mobile device. Page 3, line 16 confirms that the first part of the authorization data may comprise a PIN. Page 4, line 26 confirms that the mobile device identity information (unique identifier) may comprise the mobile telephone number. Page 11, lines 9 to 13 describe that, after (the user) has entered the PIN (into the mobile device), the Tagboard box 100 then requests the phone number from the phone. Subsequently, the Tagboard box 100 sends the PIN and the phone number to the Tagboard server. Clearly, the client device (Tagboard box 100) receives firstly the PIN and then receives the first part of the authorization data. One of ordinary skill in the art would readily appreciate that the description conveys this information to a skilled person such that they can put it into effect, i.e. that the first part of the authorization data (PIN) is received separately from the mobile device identity information (phone number). Claim 39 has, however, been amended to recite "receive separately" by way of clarifying the scope of the claim.

Furthermore, the foregoing supports claim 40 which relates to the situation where the client device (Tagboard box 100) is adapted to issue a request to the mobile device requesting the mobile device identity information in response to receiving the first part of the authorisation data from the mobile device.

Rejections under 35 USC 102(b)

The Examiner has rejected claim 14 as being anticipated by Adams et al (US2002/0181710).

Claim 14 has been amended to render it consistent with claim 1 to the effect that it now recites that "the at least one client device is adapted to receive from a mobile device identity information for said mobile device and a first part of the authorisation data" and that "the at least one server device is adapted to store said mobile device identity information and said authorisation data including a second part of the authorisation data comprising financial data relating to a user of the mobile device and, in response to receiving said first part of the authorisation data and the mobile device identity information, to verify said authorisation data and to retrieve said second part of the authorisation data comprising the user's financial data to complete a transaction" (emphasis added to identify changes).

The Examiner has indicated her view in connection with her rejection of claim 1 (under 35 U.S.C. 103(a)) that Adams teaches the feature of identity information for said mobile device being received at the point of sale 'POS' device. This is not, in fact, correct and is significant not only with respect to 35 U.S.C. 102(b), but also 35 U.S.C. 103(a) for the following reasons.

Adams teaches that a customer (user) identifies himself at the POS using an ID number previously assigned to him (paragraph 0122). This is not the same as identity information for the mobile device as will become apparent. No matter what form the ID takes or how it is delivered by the customer to the POS (see paragraphs 0123 to 0125), it is apparent that the ID identifies the customer himself and not his mobile device per se. This is most apparent from paragraph 0135 which teaches that, where an imposter not having possession of the customer's mobile phone but somehow having possession of the customer's ID is attempting to conduct an unauthorized transaction, the system

will defeat the imposter. Clearly, if the identify information taught by Adams was identity information for the mobile device rather than the customer himself then it would be of no consequence that the imposter did not have possession of the customer's phone because the imposter could arrange his own phone to convey the real customer's mobile phone identity information at the POS thereby successfully impersonating the real customer's mobile phone.

Consequently, Adams does not teach providing identity information for the mobile phone to the POS (client device) and thus claim 14 is not anticipated by Adams.

Rejections under 35 USC 103(a).

On the question of obviousness of claim 14 in light of the disclosure of Adams, Applicant makes the following observations.

As already indicated, Adams teaches that that a customer (user) identifies himself at the POS using an ID number previously assigned to him (paragraph 0122). As described in paragraphs 0123 to 0125, in most instances the customer must either memorise or have easy access to his customer ID. This may comprise a barcode applied to his mobile phone or some other audio or visual feature applied to the phone. The only forms of customer ID taught by Adams that the user need not memorise are those described at the end of paragraph 0123 (radio frequency ID signal) and paragraph 0125 (generation within the phone of an arbitrary number), but, as will be demonstrated below, the user is still required to somehow recognize or easily access such customer ID as part of the transaction authorization process.

In the case where an imposter not having possession of the customer's phone but somehow having possession of the customer's ID seeks to perform a transaction at a POS, the imposter will be thwarted by the fact that the process taught by Adams requires a second communication to be sent from the CRC to the customer's mobile phone over a wireless cellular network (paragraphs 0126 to 0136).

In the transaction process of Adams, a customer (or an imposter), as a preliminary step, provides the customer's ID to the POS (paragraph 0122). Once the customer's ID has been verified thereby verifying the customer's alleged presence at the POS (but which could be an imposter), the POS sends to the CRC a first

communication comprising transaction details consisting of the merchant's ID, the customer's ID and the transaction amount. Subsequently, in order to obtain transaction authorization from the customer, the CRC sends a second communication to the customer's mobile phone over a cellular wireless network. This second communication comprises the transaction details, namely the merchant's ID, the customer's ID and the transaction amount. Where the customer is indeed attempting to make a genuine purchase, the customer, upon receiving the anticipated second communication and then viewing the transaction details, provides authorization by accepting the transaction, which acceptance is conveyed back to the CRC as a third communication over the cellular wireless network. Presumably, the purpose of including all of the transaction details including the merchant's ID, the customer's ID and the transaction amount is so that a genuine customer can check each part to see if it is correct. The customer must therefore either somehow recognize (have memorized) or have easy access to said transaction details in order to spot any discrepancies which might require the customer to decline authorization pending correction of the transaction. Easy access implies easy accessibility for non-authorised persons and having to memorise difficult data is known to encourage people to write down in accessible places such information as an aide memoir thus putting the security of the information at risk which is clearly not desirable.

In the case that an imposter is attempting to make a transaction using a customer's ID, but not having the customer's mobile phone (paragraph 0132), the sending by the CRC of the second communication via the cellular wireless network will thwart the imposter because this message will be received at the genuine customer's mobile device who naturally will not authorize the transaction. However, this solution to the problem of imposters creates a security risk in that it requires the transaction details including the customer's ID to be transmitted over a public cellular wireless network thereby risking said information being intercepted. This is not desirable because, as is recognized in Adams, paragraph 0123, lines 4/5, it is desirable to keep one's customer ID secret.

Adams clearly and unambiguously teaches a system which attempts to verify a customer's physical presence at a POS and which seeks customer's authorization of a

transaction by sending transaction details including the customer's ID to the customer's mobile device over a public cellular wireless network.

In contrast, the present application teaches a system that verifies the presence of a mobile device at the location of client device (POS) and does not suffer the disadvantage of conveying secret customer IDs over a public communication network in a transaction authorization process. Although in exemplary embodiments of the present case, the mobile device identity information is described as being the mobile phone telephone number, one of ordinary skill in the art will appreciate that any identifier of the device such as its SIM card number could be used to uniquely identify the mobile device per se. Furthermore, there is no requirement for a user to memorise the mobile device identity information or to have easy access to it at any time, because the identity information is, as defined in claim 14, provided to the client device by the mobile device and the transaction authorization process does not require said mobile device identity information to be somehow conveyed back to the mobile device to enable a user to authorize a transaction. Consequently, the arrangement defined by claim 14 defines a more secure arrangement than that taught by Adams and, in any event, addresses a different situation despite the apparent similarities, namely that the present case is concerned with verifying the presence of a mobile device at the location of a client device (POS) whereas Adams is concerned with verifying the presence of a customer at the POS rather than the presence of the customer's mobile phone itself.

It should also be apparent that one skilled in the art would not seriously contemplate modifying the system taught by Adams by any of the other references of record to arrive at the invention as defined by claim 14 given that Adams consistently and unambiguously teaches a system where a customer's physical presence at a POS is verified and not the physical presence of his mobile phone as is required in the present application.

In summary, Adams teaches a system where it is not necessary to have possession of a customer's mobile phone physically at the location of the POS to verify the (alleged) presence of the customer at the POS, but where, in order to defeat imposters, the system sends an authorization request including the customer's ID to the customer's mobile phone over a public wireless communication network. The present

case does require the physical presence of the mobile device at the location of the client device (POS), but does not require the sending of the mobile device identity information over a public communication network to the mobile device as part of a transaction authorization process. This is because the server system stores the data relating to the mobile device identity information that enables the transaction autorisation process without recourse to communication over a public network with the mobile device thereby maintaining security of the data used in the authorization process.

It is respectfully submitted therefore that claim 14 defines an invention that is neither anticipated not rendered obvious by Adams or by any of the references of record, whether taken singly or in any combination.

It will be apparent that Applicant considers that claim 1 is not rendered obvious by the combination of Adams and Short for much the same reasons as submitted in respect of claim 14.

Remaining independent claims have each been amended to incorporate the feature of "mobile device identity information" and thus are respectfully considered as being novel and inventive over the references of record.

<u>Claims 39 and 40.</u>

The combination of Adams and Shore does not teach the use of mobile device identity information. Thus, claims 39 and 40 (as well as new claims 44 and 45, by virtue of their dependency on claim 40) are allowable over this combination of references.

Favorable reconsideration of the claims is therefore solicited.

Respectfully submitted,

Date: 23 July 2008 By: /Stephen L Grant,RegNo33390/

Stephen L. Grant, Reg No 33390
Standley Law Group LLP
495 Metro Place South, Suite 210
Dublin, Ohio 43017-5319
Telephone: (614) 792-5555
Facsimile: (614) 792-5536
E-mail: sgrant@standleyllp.com